Groups

Based on Lectures and "Algebra and Geometry"

$\theta\omega\theta$

Not in University of Cambridge
skipped some takes irrelevant to contents

E-mail: not telling you

Contents

I Groups and Permutations 1

1 Definition of Groups 1

2 Properties of Groups 1

3 Homomorphisms 3
- 3.1 Definition and basic properties 3
- 3.2 Images and Kernels 3

4 Direct product of groups 4

5 Important Examples 5
- 5.1 Cyclic groups 5
- 5.2 Dihedral Groups 6
- 5.3 Presentation 6
- 5.4 Permutation groups 7

6 Möbius group 10

7 Lagrange's Theorem 12
- 7.1 Cosets 12
- 7.2 An application in Number Theory 13
- 7.3 Exploring groups using Lagrange theorem 14
- 7.4 Studying small groups using Lagrange's Theorem 14

8 Quotient groups 15
- 8.1 Normal subgroups 15

PART

I

Groups and Permutations

1 Definition of Groups

Definition 1.1 (Group). A group is a set G together with a binary operation $* : G \times G \to G$ that

1. (Closure) $\forall g, h \in G, g * h$,
2. (Identity)$\exists e \in G, \forall g \in G, e * g = g * e = g$,
3. (Inverse)$\forall g \in G, \exists g^{-1} \in G, g * g^{-1} = g^{-1} * g = e$,
4. (Associativity)$\forall g, h, k \in G, (g * h) * k = g * (h * k)$.

Remark. The inverse of g is unique, for if there are two g', g'', both are inverses of g, we have

$$g' = g'' * g * g' = g''.$$

Example. (1) $G = \{e\}$, the trivial group,

(2) $G = \{\text{symmetries of } \triangle\}$,

(3) $(\mathbb{Z}, +)$,

(4) $(\mathbb{R}, +), (\mathbb{Q}, +), (\mathbb{C}, +)$,

(5) $\mathbb{R}^* = \mathbb{R} \setminus \{0\}\,; (\mathbb{R}^*, \times)$,

(6) $(\mathbb{Z}_n, + \pmod n), \mathbb{Z}_n = \{0, 1, \ldots, n-1\}$,

(7) Vector spaces with addition of vectors,

(8) $(\mathrm{GL}_2(\mathbb{R}), \text{matrix multiplication})$, set of invertible 2×2 matrices,

Example (non-examples). (1) $(\mathbb{Z}_n, +)$, since it is not closed,

(2) $(\mathbb{Z}, \times)$, since some inverses do not exist,

(3) $(\mathbb{R}, *)$, where $r * s = r^2 s$, since there is no identity,

(4) $(\mathbb{N}, *), n * m = |n - m|$. Associativity fails.

Here $\mathbb{N}$ is the set of all positive numbers, and it remains this definition unless specified otherwise.

2 Properties of Groups

Proposition 2.1. Let G be a group, then we have

1. The identity is unique.
2. THe inverse is unique.
3. $gh = g \wedge hg = g \Rightarrow h = e$.
4. $gh = e \Rightarrow hg = e, h = g^{-1}$.

5. $(g^{-1})^{-1} = g$.

Definition 2.1. A group G is called *abelian* if $\forall g, h \in G, gh = hg$.

Definition 2.2. G is said to be *finite* if it has finitely may elements. Denote $|G|$ as its number of elements.

Definition 2.3. Let $(G, *)$ be a group. A subset $H \subseteq G$ is called a *subgroup* of G if $(H, *)$ is a group, written as $H \leqslant G$.

Remark. To check $H \leqslant G$, simply check closure, identity, and inverses. Associativity is inherited.

Proposition 2.2. Let e_H, e_G be the identities in H and G respectively, then $e_H = e_G$.

Example. (1) $\{e\} \leqslant G$.

(2) $G \leqslant G$.

(3) $(\mathbb{Z}, +) \leqslant (\mathbb{Q}, +) \leqslant (\mathbb{R}, +) \leqslant (\mathbb{C}, +)$.

Lemma 2.1 (subgroup test)**.** Let G be a group, then $H \leqslant G \Leftrightarrow H \neq \varnothing \wedge \forall a, b \in H, ab^{-1} \in H$.

Proof. Since $gg^{-1} = e \in H$, identity is satisfied. Since $\forall a, b \in H, a(b^{-1})^{-1} = ab \in H$, closure is satisfied. $\forall g \in H, eg^{-1} = g^{-1} \in H$, inverse is satisfied. □

Proposition 2.3. The subgroups of $(\mathbb{Z}, +)$ are precisely $(n\mathbb{Z}, +)$.

Proved by considering the minimal element.

Usual laws:

Proposition 2.4. (1) Let H, K be subgroups of G then $H \cap K \leqslant G$.

(2) $K \leqslant H \wedge H \leqslant G \Rightarrow K \leqslant G$.

(3) $K \subseteq H, H \leqslant G, K \leqslant G \Rightarrow K \leqslant H$.

Definition 2.4. If $X \neq \varnothing$ is a subset of group G, the subgroup *generated* by X, written as $\langle X \rangle$, is the intersection of all subgroups containing X.

Remark.

- $e \in \langle X \rangle$.
- $X \subseteq \langle X \rangle$.
- $\langle X \rangle$ contains all possible products of elements of X and their inverses.

Proposition 2.5. Let $\varnothing \neq X \subseteq G$. Then $\langle X \rangle$ is the set of elements of G of the form

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_k^{r_k}, \quad x_i \in X, \alpha_i \in \{-1, 1\}, k \geqslant 0.$$

Proof. Let T be such a set. Then by definition $T \subseteq \langle X \rangle$. On the other hand, $X \subseteq T \Rightarrow \langle X \rangle \subseteq T$ since T clearly forms a subgroup. Hence $T = \langle X \rangle$. □

3 Homomorphisms

3.1 Definition and basic properties

Definition 3.1. Let $(G, *_G), (H, *_H)$ be groups. A function $\varphi : H \to G$ is a *homomorphism* if

$$\forall a, b \in H, \varphi(a *_H B) = \varphi(a) *_G \varphi(b).$$

It is called an *isomorphism* if it is bijective.

Proposition 3.1. Let $\varphi : H \to G$ be a homomorphism.

(1) $\varphi(e_H) = e_G$.

(2) $\varphi(h^{-1}) = \varphi(h)^{-1}$.

(3) If $\psi : G \to K$ is also a homomorphism, then $\psi\varphi : H \to K$ is a homomorphism.

Proposition 3.2. Let $\varphi : H \to G$ be an isomorphism. Then φ^{-1} is also an isomorphism and this implies that

$$G \cong H \iff H \cong G.$$

3.2 Images and Kernels

Lecture 4.

Definition 3.2. The *image* of a homomorphism $\varphi : H \to G$ is

$$\operatorname{Im}(\varphi) = \{g \in G : \exists h \in H, \varphi(h) = g\}.$$

The *kernel* of φ is

$$\ker(\varphi) = \{h \in H : \varphi(h) = e_G\}.$$

We have two immediate consequences:

Proposition 3.3. $\operatorname{Im}(\varphi), \ker(\varphi)$ are subgroups of G, H respectively.

Proof. Take $\operatorname{Im}(\varphi)$ as an example. Use lemma 2.1: $\operatorname{Im}(\varphi)$ is non-empty since $\varphi(e_H) = e_G$. For any $a, b \in \operatorname{Im}(\varphi)$, we have $a = \varphi(h), b = \varphi(h')$ for $h, h' \in H$. Hence

$$ab^{-1} = \varphi(h)\varphi(h')^{-1} = \varphi(hh'^{-1}) \in \operatorname{Im}(\varphi).$$

Hence $\operatorname{Im}(\varphi)$ is a subgroup. It is similar for $\ker(\varphi)$. □

Example. (0) Let $\varphi : H \to G$ be the trivial homomorphism, i.e. $\varphi(h) \equiv e_G$. Then $\operatorname{Im}(\varphi) = \{e_G\}$ and $\ker(\varphi) = H$.

(1) Let $\iota : H \to G$, where $H \leqslant G$, be the inclusion map. Then $\operatorname{Im}(\iota) = H, \ker(\iota) = \{e_H\}$.

(2) $\varphi : \mathbb{Z} \to \mathbb{Z}_n, \varphi(k) = k \pmod n$. $\operatorname{Im}(\varphi) = \mathbb{Z}_n, \ker(\varphi) = n\mathbb{Z}$.

Proposition 3.4. Let $\varphi : H \to G$ be a homomorphism.

(1) φ is surjective if and only if $\operatorname{Im}\varphi = G$,

(2) φ is injective if and only if $\ker\varphi = \{e\}$.

Proof. By definition, (1) holds.
Suppose φ is injective. Take $h \in \ker\varphi$. Then $\varphi(h) = \varphi(e) = e_G \Leftrightarrow h = e$. Conversely suppose $\ker\varphi = \{e\}$. Take a, b such that $\varphi(a) = \varphi(b)$. We have

$$\varphi(ab_{-1}) = \varphi(a)\varphi(b)^{-1} = e_G.$$

Thus $ab^{-1} = e_G \Leftrightarrow a = b$ and φ is injective. □

4 Direct product of groups

Definition 4.1. The *direct product* of two groups G, H is the set $G \times H$ with the operation of component-wise composition:

$$(g_1, h_1) * (g_2, h_2) := (g_1 *_G g_2, h_1 *_H h_2).$$

Closure and identity are easily verified. The inverse is component-wise and associativity is inherited from G, H.

Remark. $G \times H$ contains subgroups isomorphic to G and H, i.e., $G \times \{e_H\}$ and $\{e_G\} \times H$.

Example. $\mathbb{Z} \times \{-1, 1\}$ has elements $(n, \pm 1), n \in \mathbb{Z}$ with $(n, -1) * (m, -1) = (n + m, (-1)(-1)) = (n + m, 1)$, etc. Addition in the first component and multiplication in the second.
The identity of $\mathbb{Z} \times \{-1, 1\}$ is $(0, 1)$.

Remark. In $G \times H$, everything in (the isomorphic copy of) G *commutes* with everything in (the isomorphic copy of) H. That is to say,

$$\forall (g, e_H), (e_G, h), (g, e_H) * (e_G, h) = (e_G, h) * (g, e_H) = (g, h).$$

Theorem 4.1 (Direct Product Theorem). Let $H, K \leqslant G$ such that

(1) $H \cap K = \{e\}$: they are *disjoint*,

(2) $\forall h, k, hk = kh$: they are *commutative*,

(3) $\forall g \in G, \exists h \in H, k \in K, g = hk$: $G = HK$.

Then $G \cong H \times K$.

This gives us two ways to think about direct products:

- Given two groups H, K, one can form their direct products $H \times K$ and view H, K as subgroups via $H \times \{e_K\}$ and $\{e_H\} \times K$.
- Given a group G with subgroups H, K that satisfiy these conditions, then we are equivalently dealing with $H \times K$.

By convention, we can simply regard $H \times \{e_K\}, \{e_H\} \times K$ as H, K.

Proof. Consider the function $\varphi : H \times K \to G$ defined by $\varphi(h, k) = hk$. Note that

$$\varphi(h, k) * \varphi(h', k') = hkh'k' = hh'kk' = \varphi(hh', kk') = \varphi((h, k) * (h', k')),$$

so φ is a homomorphism. From (3) we know that φ is surjective. Let $\varphi(h, k) = e$, then $hk = e \Leftrightarrow h = k^{-1}$. Hence $h, k^{-1} \in H \cap K$ so $h = k = e$. Hence it is injective. Thus φ is an isomorphism and $G \cong H \times K$. □

5 Important Examples

5.1 Cyclic groups

Definition 5.1. Let G be a group and let $X \subseteq G, X \neq \varnothing$. If $\langle X \rangle = G$, then X is called *a generating set*[1] of G.
G is *cyclic* if $\exists a \in G$ such that $\langle a \rangle = G$. In this case, $\forall b \in G, \exists k \in \mathbb{Z}, b = a^k$. a is called a *generator* of G.

[1] *It is not necessary unique.*

Example. (0) Trivial group $\{e\} = \langle e \rangle$.

(1) $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$.

(2) $(\mathbb{Z}_n, +_n) = \langle 1 \rangle = \langle k \rangle$, where $(k, n) = 1$.

(3) $E = \left(\left\{e^{\frac{2\pi i k}{n}} : 0 \leqslant k \leqslant n-1\right\}, \cdot\right) = \langle e^{\frac{2\pi i m}{n}} \rangle$, where $(m, n) = 1$.

Hence, $E \cong \mathbb{Z}_n$.

(4) $\{e, a, a^2, \ldots, a^{n-1}\}$ with

$$a^k * a^j = \begin{cases} a^{k+j} & \text{if } k+j < n, \\ a^{k+j-n} & \text{if } k+j \geqslant n. \end{cases}$$

Again, it is isomorphic to $\mathbb{Z}_n$.

Write $C_n = \{e, a, a^2, \ldots, a^{n-1}\}$. Then every cyclic group is isomorphic to C_n and we can write all cyclic groups in this form, or $\cong \mathbb{Z}$, which is the infinite case.

Lecture 5

Theorem 5.1. A cyclic group G is isomorphic to $\mathbb{Z}$ or C_n for some $n \in \mathbb{N}$.

Therefore we often write $\mathbb{Z}$ or C_n for a cyclic group, regardless of its description.

Proof. Let $G = \langle b \rangle$. Suppose that $\exists n, b^n = e$. Take the smallest n. Define $\varphi : C_n = \{e, a, a^2, \ldots, a^{n-1}\} \to G$ by $\varphi(a^k) = b^k (0 \leqslant k \leqslant n-1)$. Then $\forall a^j, a^k \in C_n, j, k < n$, we have

$$\varphi(a^j \cdot a^k) = \varphi(a^{j+k}) = b^{j+k} = b^j * b^k = \varphi(a^j) * \varphi(a^k).$$

If $j + k \geqslant n$,

$$\varphi(a^j \cdot a^k) = \varphi(a^{j+k-n}) = b^{j+k-n} = b^{j+k} * (b^n)^{-1} = b^{j+k} = \varphi(a^j) * \varphi(a^k).$$

Hence φ is a homomorphism. Since $b^n = e$, φ is surjective. Suppose $\varphi(a^k) = e \Leftrightarrow b^k = e \Leftrightarrow k = 0$, since $0 \leqslant k \leqslant n-1$. Otherwise $\#$ to minimality of n.
If no such n exists, then define $\varphi : \mathbb{Z} \to G$ ny $\varphi(k) = b^k$. Note that

$$\varphi(k + m) = b^{k+m} = b^k * b^m = \varphi(k) * \varphi(m).$$

Also $\forall b^k \in G = \langle b \rangle, \varphi(k) = b^k$, and if $m \in \ker \varphi$, then $\varphi(m) = e = b^m \wedge \varphi(-m) = e$.
If $m \neq 0$, then $\#$ to the assumption that $\nexists n, b^n = e$.
Therefore, $G \cong \mathbb{Z} \vee G \cong C_n$. □

Definition 5.2. The *order of an element* $g \in G$ is the smallest $n \in \mathbb{N}$ that $g^n = e$. If no such n exists, we say g has and *infinite order*. The order of g is written as $\operatorname{ord} g$.

Proposition 5.1. If $g^m = e, m > 0$, then $\operatorname{ord} g | m$.

Proof. If not, then $m = q \operatorname{ord} g + r$ for some $q, r \in \mathbb{N}$ such that $0 \leqslant r \leqslant \operatorname{ord} g - 1$, #. □

Remark. Given $g \in G$, the subgroup $\langle g \rangle \cong C_n$ if $\operatorname{ord} g = n$, and $\cong \mathbb{Z}$ if $\operatorname{ord} g = \infty$. Hence $\operatorname{ord} g = |\langle g \rangle|$.

Proposition 5.2. Cyclic groups are abelian.

5.2 Dihedral Groups

Definition 5.3. The *dihedral group* D_{2n} is the group of symmetries of a regular n-gon, the operation is composition of symmetries.

Example. D_6 = symmetries of $\triangle$.

What are the elements of D_{2n}?
Clearly we have n rotations of angles

$$\frac{2\pi k}{n}, \quad 0 \leqslant k < n.$$

- When n is odd, we have n reflections in axes through the centre and each of the vertices.
- When n is even, we have $n/2$ reflections in axes through centre and pairs of opposite vertices. Another $n/2$ reflections in axes through pairs of opposite mid-points of edges.

Assert that these are all the elements of D_{2n}. Indeed, let $g \in D_{2n}$. Since g is a symmetry, then g must send vertices to vertices, e.g., $g(v_1) = v_i$. g must also send edges to edges, so v_2, v_n must be sent to $\{v_{i-1}, v_{i+1}\}$. Note that once we know where $g(v_1), g(v_2)$, then $g(v_n)$ is determined. *Inductively*, all other $g(v_j)$ are determined, and hence g is known. Since there are n choices for v_1 and 2 choices for v_2, so we have $2n$ elements in total. Hence there are no other elements.

It can be checked easily that D_{2n} is a group.

Remark. Can generate D_{2n} by a rotation and a reflection. Let r be the rotation $\frac{2\pi}{n}$ and s be the reflection in axis through v_1 and centre, then r^k give all rotations. Consider $r^i s r^{-i}$:

$$\begin{aligned} r^i s r^{-i} : & v_{i+1} \mapsto v_1 \mapsto v_1 \mapsto v_{i+1}, \\ & v_{i+2} \mapsto v_2 \mapsto v_n \mapsto v_i, \\ & v_i \mapsto v_n \mapsto v_2 \mapsto v_{i+2} \mapsto v_{i+2}. \end{aligned}$$

The form $r^i s r^{-i}$ is called *conjugation* and allows us to change the axis of operation.

We get reflection in axis through v_{i+1} and centre. If n is even, consider

$$\begin{aligned} r^{i+1} s r^{-i} : & v_{i+1} \mapsto v_1 \mapsto v_1 \mapsto v_{i+2}, \\ & v_{i+2} \mapsto v_2 \mapsto v_n \mapsto v_{i+1}. \end{aligned}.$$

Hence they give all symmetries and $D_{2n} = \langle r, s \rangle$ and $rs = sr^{-1}$, so it is not abelian.

5.3 Presentation

One way to write groups is via a *presentation*:

$$\langle \text{generators} | \text{relation between generators} \rangle.$$

For example, $C_n = \langle a | a^n = e \rangle$, and $D_{2n} = \langle r, s | r^n = e, s^2 = e, rs = sr^{-1} \rangle$.

Should be able to deduce all the properties in the group from the relatios in the presentation. In general it is not easy to write down a presentation for a given group, or to determine the group from a given presentation. E.g.,

$$\langle a,b,c|aba^{-1}b^{-1}=b, bcb^{-1}c^{-1}=c, cac^{-1}a^{-1}=a\rangle$$
$$\langle a,b,c,d|aba^{-1}b^{-1}=b, bcb^{-1}c^{-1}=c, cdc^{-1}d^{-1}=d, dad^{-1}a^{-1}=a\rangle$$

The first group is simply $\{e\}$ but the second group, known as Higman group, is very non-trivial.

5.4 Permutation groups

Definition 5.4. Given a set X, a *permutation* of X is a bijective function $\sigma : X \to X$. The set of all permutations of X is denoted by $\operatorname{Sym} X$.

Of course we have

Theorem 5.2. $\operatorname{Sym} X$ forms a group wrt compositions.

Definition 5.5. If $|X| = n$, we write S_n for (the isomorphism class of) $\operatorname{Sym} X$. S_n is called *symmetric group* on n elements.

Remark. $|S_n| = n!$. Usually use $X = \{1, 2, \ldots, n\}$ to study S_n.

One way to write permutations is using a two-row notation. For example, consider $\sigma \in S_3$ such that $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$ can be represented as

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

In general, write $\sigma \in S_n$ as

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}.$$

Given a permutation that "cycles" some elements $a_1, \ldots, a_k \in \{1, 2, \ldots, n\}$ and leaves the other unchanged, then we can write as

$$(a_1 a_2 \ldots a_k) = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_k \\ \sigma(a_1) & \sigma(a_2) & \sigma(a_3) & \cdots & \sigma(a_k) \end{pmatrix}.$$

So in general,

$$(a_1 \ldots a_k)(x) = \begin{cases} a_{i+1} & \text{if } x = a_i (i < k) \\ a_1 & \text{if } x = a_k \\ x & \text{otherwise.} \end{cases}$$

Note that $(a_1 \ldots a_k) = (a_2 \ldots a_k a_1) = \cdots$.

Definition 5.6. A permutation of the form $\sigma = (a_1 \ldots a_k)$ is called a *k-cycle*. If $k = 2$ then it is called a *transposition*.

Example. (1). Consider (1234)(324). $1 \mapsto 2$, $2 \mapsto 1$, $3 \mapsto 3$, $4 \mapsto 4$. Hence

$$(1234)(324) = (12).$$

(2). In S_5, $(254)(534) = (1)(253)(4) = (253)$.

Remark. (1). The inverse of $(a_1 \dots a_k)$ is $(a_k a_{k-1} \dots a_1)$.

(2). $S_3 = D_6$, but in general $D_{2n} \leqslant S_n$.

Definition 5.7. (1). Two cycles are *disjoint* if no element appears in both of them.

(2). $g, h \in G$ are *commute* if $gh = hg$ in G.

Lemma 5.3. Disjoint cycles commute.
Note that S_n is non-abelian for $n \geqslant 3$.

Proof. Let $\sigma, \tau \in S_n$ such that σ, τ are disjoint. Let $x \in \{1, 2, \dots, n\}$.
If x is in neither of σ, τ, then $\sigma\tau(x) = \tau\sigma(x)$. If $x \in \tau$ but not in σ, then $\tau(x) \in \tau \notin \sigma$, so $\sigma\tau(x) = \tau\sigma(x) = \tau(x)$. Similar for $x \in \sigma, x \notin \tau$. □

Theorem 5.4. Any $\sigma \in S_n$ can be written as a composition of disjoint cycles, and this representation is unique up to reordering cycles, and "cycling" of cycles.

Proof. Take $\sigma \in S_n$ and consider $1, \sigma(1), \sigma^2(1), \dots$. Since $\{1, 2, \dots, n\}$ is finite, $\exists a > b$, $\sigma^a(1) = \sigma^b(1)$, so that $\sigma^{a,b}(1) = 1$. Let k be the smallest integer that $\sigma^k(1) = 1$. Then $\forall l > m \in [0, k]$, if $\sigma^l(1) = \sigma^m(1)$ then $\sigma^{l-m} = 1$, contradicting with the minimality of k, so $1, \sigma(1), \dots, \sigma^{k-1}(1)$ are distinct. This cycle

$$\Big(1 \ \sigma(1) \ \sigma^2(x) \ \cdots \ \sigma^{k-1}(1)\Big)$$

is the first cycle in decomposition. We can repeat this with the next number in $\{1, 2, \dots, n\}$ that has not already appeared.
Since σ is a bijection, no number can reappear. Continue with this we exhaust $\{1, 2, \dots, n\}$ and we get

$$\Big(1 \ \sigma(1) \ \cdots \ \sigma^{k-1}(1)\Big)\Big(a \ \sigma(a) \ \cdots \ \sigma^{k-1}(a)\Big) \cdots .$$

Hence it exists. To show it is unique, suppose we have to decompositions:

$$\begin{aligned} \sigma &= \Big(a_1 \ \cdots \ a_{k_1}\Big)\Big(a_{k_2} \ \cdots \ a_{k_3}\Big) \cdots \Big(a_{k_{n-1}} \ \cdots \ a_{k_n}\Big) \\ &= \Big(b_1 \ \cdots \ b_{l_1}\Big)\Big(b_{l_2} \ \cdots \ b_{l_3}\Big) \cdots \Big(b_{l_{s-1}} \ \cdots \ b_{l_s}\Big), \end{aligned}$$

so each $j \in \{1, 2, \dots, n\}$ appears exactly once in both. Then we have $a_1 = b_t$ for some t, and the other numbers appearing in the cycle of b_t are uniquely determined by $\sigma(a_1), \sigma^2(a_1), \dots$. So

$$\Big(a_1 \ \cdots \ a_{k_1}\Big) \cdots = \Big(b_t \ \cdots\Big) \cdots$$

since disjoint cycles commute and we can cycle cycles. Continue in this way, we see that all other cycles match. □

Definition 5.8. The set of cycle lengths of the disjoint cycle decomposition of σ is its *cycle type* of σ.

Lecture 7

Example. (123)(56) has cycle type 3,2(or 2,3).

Theorem 5.5. The order of $\sigma \in S_n$ is the lcm of the cycle length in its cycle type.

Proof. Firstly note that the order of a k-cycle is k. Suppose $\sigma = \tau_1\tau_2 \cdots \tau_r$, where τ_i are disjoint cycles, we have

$$\sigma^m = \tau_1^m \tau_2^m \cdots \tau_r^m,$$

since disjoint cycles commute. Let each τ_i be a k_i-cycle, then if $\sigma^m = e$, we have $\tau_1^m, \tau_2^m, \dots, \tau_r^m = e$, and so $\tau_1^m = \tau_2^{-m}\tau_3^{-m} \cdots \tau_r^{-m}$. The numbers permuted by LHS and RHS are disjoint since τ_i are disjoint, so LHS, RHS must be e. So $\tau_1^m = e$ and $k_1|m$.
This holds for any k_i and $k_i|m$, so $l = \operatorname{lcm}(k_1, \dots, k_r) | \operatorname{ord}(\sigma)$. But if we take

$$\sigma^l = \tau_1^l \tau_2^l \cdots \tau_r^l = \prod_{i=1}^{r} (\tau^{k_i})^{l/k_i} = e.$$

So $\operatorname{ord}(\sigma) = \operatorname{lcm}(k_1, \dots, k_r)$. □

Remark. Disjoint cycle notation allows us to quickly compare elements of S_n, and to read off their orders.

Disjoint cycle notation is just one useful way to express elements of S_n. Another is as a product of transpositions:

Proposition 5.3. Let $\sigma \in S_n$, then σ is a product of transpositions.

Proof. By theorem 5.4, it's enough to do this for a cycle. We observe that

$$(a_1 a_2 a_3 \cdots a_k) = (a_1 a_2)(a_2 a_3) \cdots (a_{k-1} a_k).$$

□

Remark. This is not unique. e.g., (1234)=(12)(23)(34)=(12)(23)(12)(34)(12). But the *parity* of the numbers of transpositions is well-defined..

Theorem 5.6. Writing $\sigma \in S_n$ as a product of transpositions in different ways, σ is either always a product of an even number of transpositions, or always a product of an odd number of transpositions.

Proof. Write $\#(\sigma)$ for the number of cycles in σ in disjoint cycle decompositions, including any one-cycles. For example, $\#((12)(34)) = \#((123)) = 2, \#(e) = 4$. Let's see what happens to $\#(\sigma)$ if we multiply σ by a transposition $\tau = (cd)$.

- This will not affect any cycles not including c or d.
- If c, d are in the same cycle in (disjoint cycle decomposition) of σ, say $(c a_2 a_3 \cdots a_{k-1} d a_{k+1} \cdots a_l)$, then

$$(c a_2 a_3 \cdots a_{k-1} d a_{k+1} \cdots a_l)(cd) = (c a_{k+1} a_{k+2} \cdots a_l)(d a_2 \cdots a_{k-1}),$$

so $\#(\sigma\tau) = \#(\sigma) + 1$.

- If c, d are in different cycles (possibly 1-cycle),

$$(ca_2 \cdots a_k)(db_2 \cdots b_l)(cd) = (cdb_2 \cdots b_l dca_2 \cdots a_k).$$

So $\#(\sigma\tau) = \#(\sigma) - 1$.

So far any σ and any transposition τ, $\#(\sigma) \equiv \#(\sigma\tau) + 1 \pmod 2$. Now suppose σ is written as 2 different products of transpositions

$$\sigma = \tau_1 \cdots \tau_k = \tau_1' \ldots \tau_l'.$$

We know by the previous theorem that $\#(\sigma)$ is uniquely determined by σ. Also we have

$$\sigma = e \cdot \tau_1 \cdots \tau_k = e \cdot \tau_1' \ldots \tau_l',$$

and so applying the above several times, we get

$$\#(\sigma) \equiv \#(e) + k \equiv n + k \pmod 2; \#(\sigma) \equiv \#(e) + l \equiv n + l \pmod 2.$$

So $n + k \equiv n + 2 \pmod 2 \Leftrightarrow k \equiv l \pmod 2$. Hence k, l has the same parity. □

Definition 5.9. Writing $\sigma \in S_n$ as a product of transositions, $\sigma = \tau_1 \cdots \tau_k$, the *sign* of σ is defined as $\epsilon(\sigma) = (-1)^k$. If $\epsilon(\sigma) = 1$, we say σ is an *even* permutation, and odd permutation if $\epsilon(\sigma) = -1$.

Theorem 5.7. For $n \geqslant 2$, the sign function $\epsilon : S_n \to \langle -1 \rangle$ is a surjective homomorphism.

Proof. If σ, σ' can be written as k, l transpositions respectively, then $\sigma\sigma'$ can be written as a product of $k + l$ transpositions and $\epsilon(\sigma\sigma') = (-1)^{k+l} = (-1)^k \cdot (-1)^l = \epsilon(\sigma) \cdot \epsilon(\sigma')$. To see it is surjective, since $n \geqslant 2$, $\epsilon(e) = 1$ and $\epsilon(12) = -1$, so it is. □

Definition 5.10. The *kernel* of the homomorphism ϵ is called the *alternating group*, $A_n \leqslant S_n$.

Proposition 5.4. $\sigma \in S_n$ is even if and only if its disjoint cycle decomposition contains an *even number* of *even* cycles.

Here "even cycle" means a cycle of even number of elements.

Proof. Write

$$\sigma = \delta_1 \delta_2 \cdots \delta_k \chi_1 \chi_2 \cdots \chi_l,$$

where δ are even cycles, and χ are odd cycles. Then $\epsilon(\sigma) = (-1)^k$ and the result follows. □

6 Möbius group

Lecture 8

The study of permutations of an infinite object, the functions $\mathbb{C} \to \mathbb{C}$. Since $\mathbb{C}$ has geometry unlike $\{1, 2, \ldots, n\}$, need to restrict to functions that interact well with this geometry.

More precisely, we want to study functions of the form

$$f : \mathbb{C} \to \mathbb{C}, \quad f(z) = \frac{az + b}{cz + d}, \quad a, b, c, d, \in \mathbb{C}$$

such that $ad - bc \neq 0$.

Note that

$$f(z) - f(w) = \frac{(ad-bc)(z-w)}{(cw+d)(cz+d)},$$

so $f(z) = f(w)$ and f would be constant. However we need invertible functions, so we do need $ad - bc \neq 0$.

f is undefined at point $-d/c$, to fix this, we introduce a new point ∞ to $\mathbb{C}$, forming the *extended complex plane* $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$. Can visualise using *stereographic projection*.

Definition 6.1. A *Möbius map* is a function $f : \hat{\mathbb{C}} \to \hat{\mathbb{C}}$ of the form

$$f(z) = \frac{az+b}{cz+d}, a, b, c, d \in \mathbb{C}, ad - bc \neq 0, f\left(\frac{-d}{c}\right) = \infty,$$

with

$$f(\infty) = \begin{cases} \frac{a}{c} & \text{if } c \neq 0, \\ \infty & \text{if } c = 0. \end{cases}$$

Lemma 6.1. Möbius maps are bijections $\hat{\mathbb{C}} \to \hat{\mathbb{C}}$.

Proof. Note that for $f(z) = \frac{az+b}{cz+d}$,

$$f^{-1}(z) = \frac{dz - b}{-cz + a},$$

which could be checked by doing some algebras. □

Theorem 6.2. The set of Möbius maps form a group M wrt composition.

Proof. Note that the identity is $z \mapsto z = \frac{1z+0}{0z+1}$, and by lemma they are invertible. Associativity is inherited from the structure of functions in $\mathbb{C}$. □

Remark. M is not abelian. e.g. take $f_1(z) = z + 1, f_2(z) = 2z$. In dealing with Möbius maps in $\hat{\mathbb{C}}$, we use the convention $\frac{1}{\infty} = 0, \frac{1}{0} = \infty, \frac{a\infty}{c\infty} = \frac{a}{c}$.

Proposition 6.1. Every Möbius group can be written as a composition of maps of the following forms:

(1) $f(z) = az (a \neq 0)$, a dilation/rotation.

(2) $f(z) = z + b$, translation.

(3) $f(z) = \frac{1}{z}$, inversion.

Proof. Let

$$f(z) = \frac{az+b}{cz+d}.$$

If $c \neq 0$, then $f(z)$ is the composition

$$z \mapsto z + \frac{d}{c} \mapsto \frac{1}{z + \frac{d}{c}} \mapsto \frac{(-ad+bc)c^{-2}}{z + \frac{d}{c}} \mapsto \frac{a}{c} + \frac{(-ad+bc)c^{-2}}{z + \frac{d}{c}} \mapsto \frac{az+b}{cz+d}.$$

If $c = 0$, $z \mapsto \frac{a}{d} z \mapsto \frac{a}{d} z + \frac{b}{d}$. □

In particular, the set S of all dilations/rotations, translations, and inversions generate M. i.e., $\langle S \rangle = M$.

7 Lagrange's Theorem

This result allows us to study the internal structure of a group wrt a subgroup.

7.1 Cosets

Definition 7.1. Let $H \leqslant G$ and $g \in G$. Let $gH = \{gh : h \in H\}$, then gH is called a *left coset* of H in G. Right coset is defined similarly.

Cosets can be thought as a "translated copy" of H that may no longer be a subgroup.

Example. (1) Let $H = 2\mathbb{Z} \leqslant \mathbb{Z}$, then some cosets are:

$0 + 2\mathbb{Z} = 2\mathbb{Z}$, all even integers,

$1 + 2\mathbb{Z}$ is all odd integers. Note that

$$n + 2\mathbb{Z} = \begin{cases} 2\mathbb{Z} & \text{if } n \text{ is even,} \\ 1 + 2\mathbb{Z} & \text{if } n \text{ is odd.} \end{cases}$$

Hence these are the only cosets of $2\mathbb{Z}$.

(2) Let $H = \{e, (12)\} \leqslant S_3$. Then $eH = H$, $(12)H = H$, $(13)H = \{(13), (123)\}$.

Somethings to notice from example (2):

- $eH = H$.
- $hH = H$ whenever $h \in H$.
- $|H| = |gH|$.
- $\bigcup_{g \in G} gH = G$.

In fact,

Lecture 9

Cosets *pave* the group.

Theorem 7.1 (Lagrange)**.** Let $H \leqslant G$ where G is finite, then

1. $|H| = |gH|$ for any $g \in G$.
2. If $g_1, g_2 \in G$, then either $g_1H = g_2H$ or $g_1H \cap g_2H = \varnothing$.
3. $\bigcup_{g \in G} gH = G$.

In particular, define the *index* of H in G to be the number of distinct cosets of H in G, denoted by $|G : H|$. Then we have

$$|G| = |G : H||H|.$$

Proof.

1. The function $\varphi : H \to gH$ defined by $\varphi(h) = gh$ for $h \in H$, is a bijection between H and gH. Surjection is obvious since every $gh = \varphi(h) \in gH$. To show its injectivity, note that $\varphi(h_1) = \varphi(h_2) \Rightarrow gh_1 = gh_2 \Rightarrow h_1 = h_2$. Therefore, $|H| = |gH|$.
2. Suppose $g_1H \cap g_2H \neq \varnothing$. Then $\exists g \in g_1H \cap g_2H \Rightarrow g = g_1h_1 = g_2h_2$, where $h_1, h_2 \in H$. This means that $g_1 = g_2h_2h_1^{-1}$, and so $\forall h \in H, g_1h = g_2h_2h_1^{-1}h \in$

$g_2H \Rightarrow g_1H \subseteq g_2H$. Similarly $g_2H \subseteq g_1H$, and so they are identical.

3. Given $g \in G$, then $g \in gH$ so $g \in \bigcup_{g\in G} gH \Rightarrow G \subseteq \bigcup_{g\in G} gH$. Certainly $\bigcup_{g\in G} gH \subseteq G$ since all are subsets. Hence

$$\bigcup_{g\in G} gH = G.$$

Since G is the distinct union of distinct cosets of H, $|G| = |G : H||H|$. $\square$

Remark. Right cosets also works, using the same arguments. However, $gH \neq Hg$ in general, since a group needs not to be abelian. For example, if $H = \{e, (12)\} \leqslant S_3$, the coset $(13)H = \{(13), (123)\}$ while $H(13) = \{(13), (132)\}$. Another fact to notice from this is that the set of cosets are not necessarily the same wrt left/right. H is particulary special and interesting if $gH = Hg$.

Proposition 7.1. $g_1H = g_2H \iff g_1^{-1}g_2 \in H$.

Proof. If $g_1H = g_2H$, then $g_1 = g_2h$ for some $h \in H$. Hence $g_1^{-1}g_2 = h^{-1} \in H$. Conversely if $g_1^{-1}g_2 \in H$, $g_1g_1^{-1}g_2 \in g_1H \Rightarrow g_2 \in g_1H$. By Lagrange's theorem, they are identical. $\square$

Take $g_1, g_2, \ldots, g_{|G:H|}$ from each disjoint coset of H in G. Then we have

$$G = \bigsqcup_{i=1}^{|G:H|} g_iH,$$

where $\bigsqcup$ is the disjoint union notation. The g_i are called *coset representation* of H in G.

Corollary 7.2. Let G be a finite group and $g \in G$, then $\mathrm{ord}(g)||G|$.

Proof. Let $H = \langle g\rangle$, then $\mathrm{ord}(g) = |H|$ and thus $\mathrm{ord}(g)||G|$ by Lagrange's theorem. $\square$

Corollary 7.3. Let G be a finite group. If $g \in G$, then $g^{|G|} = e$.

Proof. $g^{|G|} = g^{\mathrm{ord}(g)n} = e^n = e$. $\square$

Corollary 7.4. If $|G|$ is prime, then G is cyclic, and is generated by any non-identity element.

Proof. Since $|G| = p$, p is prime, then $|\langle g\rangle|||G|$ by Lagrange. Since p is prime, then $|\langle g\rangle| = 1$ or p. Hence if $g \neq e$, then $g, e \in \langle g\rangle$ so $|\langle g\rangle| = p$, and thus $\langle g\rangle = G$. $\square$

7.2 An application in Number Theory

Consider $(\mathbb{Z}_n, +_n)$. Define $a * b = ab \pmod n$. This is well-defined since $a_1 \equiv a_2 \pmod n \wedge b_1 \equiv b_2 \pmod n \Rightarrow a_1b_1 \equiv a_2b_2 \pmod n$. $(\mathbb{Z}_n, *)$ is not a group since 0 has no inverse.

Let $\mathbb{Z}_n^* \subseteq \mathbb{Z}_n$ be the subset of elements of $\mathbb{Z}_n$ that have inverses. In fact, we have

Proposition 7.2. $\mathbb{Z}_n^* = \{a \in \mathbb{Z}^n : (a, n) = 1\}$.

Proof. Let $a \in \mathbb{Z}_n$ such that a, n are coprime. Then $\exists b, m, ba + mn = 1 \Rightarrow b$ is the inverse of a and $\{a \in \mathbb{Z}^n : (a, n) = 1\} \subseteq \mathbb{Z}_n^*$.
Conversely if a has an inverse in $\mathbb{Z}_n$, then $\exists b, ab \equiv 1 \pmod n \Rightarrow \exists m, ab + mn = 1 \Rightarrow (a, n) = 1$. Hence $\mathbb{Z}_n^* \subseteq \{a \in \mathbb{Z}^n : (a, n) = 1\}$. $\square$

Obviosuly $1 \in \mathbb{Z}_n^*$. By defintion every revertible element and its inverse is in $\mathbb{Z}_n^*$. Any product of two invertible elements is invertible, so $\mathbb{Z}_n^*$ is closed under $*$. Associativity is inherited from $\mathbb{Z}_n$, so $\mathbb{Z}_n^*$ is a *subgroup* of $\mathbb{Z}_n$.

Definition 7.2 (Euler totient function)**.** $\phi(n) = |\mathbb{Z}_n^*|$.

Theorem 7.5 (Fermat-Euler)**.** Let $n \geqslant 1$, $N \in \mathbb{Z}, (N, n) = 1$, then

$$N^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof. Let $a \in \mathbb{Z}_n$ such that $N \equiv a \pmod{n}$. Then $a \in \mathbb{Z}_n^*$ and thus $a^{|\mathbb{Z}_n^*|} = a^{\phi(n)} \equiv 1 \pmod{n}$. Since $N = a + kn$,

$$N^{\phi(n)} = (a + kn)^{\phi(n)} \equiv a^{\phi(n)} \equiv 1 \pmod{n}.$$

□

Take $n = p$, we get $N^{p-1} \equiv 1 \pmod{p}$ for $(N, p) = 1$.

7.3 Exploring groups using Lagrange theorem

Lagrange tells us what the possible orders of subgroups can be.

Remark. Not all possible orders have to appear.

Example. For D_{10}, the sizes of subgroups can be $1, 2, 5, 10$. We have $|\{e\}| = 1$, $|\{e, g\}| = 2$, where g has order 2. This can be done since we have 5 reflections. For subgroups of order 5, they must be cyclic by corollary 7.4. We have $|\langle r \rangle| = 5$, where r is a rotation. Obviously $|D_{10}| = 10$.

7.4 Studying small groups using Lagrange's Theorem

Lecture 10

Example.

- $|G| = 1 \Rightarrow G = \{e\}$.
- $|G| = 2 \Rightarrow G \cong C_2$ since 2 is prime.
- $|G| = 3 \Rightarrow G \cong C_3$.
- $|G| = 4$, then $G \cong C_4$ or $G \cong C_2 \times C_2$.

  proof. By Lagrange, the possible orders of subgroups of G is $1(\{e\})$, $2(C_2)$, and 4. If $\exists g \in G, \operatorname{ord} g = 4$, then $G = \{e, g, g^2, g^3\}$ and thus $G \cong C_4$. If no element has order 4, then all non-identity elements have order 2. Claim that G is abelian. Indeed, let $h, g \in G, h, g \neq e$, then $\operatorname{ord} g = \operatorname{ord} h = 2$ and we have

  $$gh = h^2 g h g^2 = h(hg)^2 g = hg.$$

  Take $b \neq c \in G$ such that $\operatorname{ord} b = \operatorname{ord} c = 2$. Since $(\langle b \rangle \cap \langle c \rangle = \{e\}) \wedge (\forall b' \in \langle b \rangle, c' \in \langle c \rangle, b'c' = c'b') \wedge (bc \neq b \wedge bc \neq c \Rightarrow \forall g \in G, g = b'c', b \in \langle b \rangle, c' \in \langle c \rangle)$, we have $G \cong \langle b \rangle \times \langle c \rangle$ and thus $G \cong C_2 \times C_2$.
- $|G| = 5$ then $G \cong C_5$. We need more tools to study groups of order $\geqslant 6$.

8 Quotient groups

8.1 Normal subgroups

Definition 8.1. A subgroup N of G is *normal* if $\forall g \in G, gN = Ng$. Written as $N \trianglelefteq G$.

Proposition 8.1. The followings are equivalent:

(1) $\forall g \in G, gN = Ng$.

(2) $\forall g \in G, \forall n \in N, g^{-1}ng \in N$.

(3) $\forall g \in G, g^{-1}Ng = N$.

Proof. (1) $\Rightarrow$ (2). If $gN = Ng$, we have $\forall n \in N, ng \in Ng = gN \Rightarrow ng = gn'$ for some $n \in N$. Hence $g^{-1}ng = g^{-1}gn' = n \in N$.
(2) $\Rightarrow$ (3). From (2) we know that $g^{-1}Ng \subseteq N$. Suppose $n \in N$ and let $n' = gng^{-1}$, then $n = g^{-1}n'g \in g^{-1}Ng \Rightarrow g^{-1}Ng = N$.
(3) $\Rightarrow$ (1). Trivial. $\square$

Example. (1) $\{e\}$ and G are always normal.

(2) $n\mathbb{Z} \trianglelefteq \mathbb{Z}$.

(3) $A_3 \trianglelefteq S_3$, recall that A_3 is the alternating group.